IDVerifact

Information Security Policy – IT Compliance

April 07, 2021

Revision History

Update this table every time a new edition of the document is published

Date	Authored by	Title	Ver.	Notes
5/1/2019	Mark Salonius	IT Ops Manager	1.0	Initial draft
5/8/2019	Joel Massicotte	CISO	1.1	Update
4/19/2020	Sanjiv Pruba	CISO	1.2	Update
04/07/2021	Sanjiv Pruba	CISO	1.3	Reviewed and updated

Table of Contents

PART 1. PREFACE 3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES 3
PART 3. PURPOSE 3
PART 4. SECTION OVERVIEW 4

INFORMATION SECURITY POLICY 5

IT Compliance 5
1.1 Audit and Compliance Requirements 5
1.2 Information System Audit Considerations 6
1.3 Information Security Continuous Monitoring 7
IT Policy 7
1.0 Scope 7
2.0 Policy - Employee requirements 7
3.0 Workstation Full Disk Encryption 8
Scope 8
Policy 8

DEFINITIONS 9

Part 1. Preface

The IDVerifact Information Security Program consists of information security policies that establish a common information security framework across the organization.

Together these policies provide a framework for developing an agency's information security program. An effective information security program improves the organization's security posture and aligns information security with the organization's mission, goals, and objectives.

Part 2. Organizational and Functional Responsibilities

The policy sets the minimum level of responsibility for the following individuals and/or groups:

- Company Leadership and Delegates
- IT and Operations
- Employees, Contractors, and Third Parties

(A) Executive Leadership

- Ensure Policies are reviewed quarterly to ensure continued compliance
- Lead any internal change efforts required to achieve compliance, and or adopt/adapt to changes within the compliance standard
- Ensure policies are published and appropriate standards training is provided to all employees annually

(B) IT and Operations

The duties of the IT and IT Operations department are:

- Developing, maintaining, and revising information security policies, procedures, and recommended technology solutions
- Providing technical assistance, advice, and recommendations concerning information security matters

(C) Employees, Contractors and Third Parties

All IDVerifact employees, contractors, and third-party personnel are responsible for:

- Being aware of and complying with organizational policies and their responsibilities for protecting IT assets of their organization
- Using information resources only for intended purposes as defined by policies, laws and regulations of the organization
- Being accountable for their actions relating to their use of all organization information systems

Part 3. Purpose

The information security policies set forth the minimum requirements that are used to govern the IDVerifact organization. Employees and Contractors are expected to comply with the information security policy. These policies exist in addition to all other organizational policies governing the protection of the organizations data. Adherence to the policies will improve the security posture of IDVerifact information technology resources.

Part 4. Section Overview

Each information security policy section consists of the following:

- **Purpose:** Provides background to each area of the information security policies.
- **Policy:** Contains detailed policies that relate to each information security section.
- **Policy Supplement:** Contains the security solution recommendations.
- **Guidance:** Provides references to guidelines on information security policies.
- **Reference:** Provides a reference to the guidance in the form of a uniform resource locator (URL).

IT Compliance

1.1 Audit and Compliance Requirements

Purpose

The purpose of the Audit and Compliance section is to establish controls and processes to help ensure compliance of with information security policies and standards at Prodigy Labs/Prodigy Ventures.

Policy

Compliance with legal and contractual requirements

- IDVerifac tshall identify and document its obligations to applicable laws and regulations in relation to information security.

Compliance with security policies and standards

- At least annually, IDVerifact shall perform reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.
- Results from compliance reviews or audits shall be documented and reported to IDVerifact leadership.

Audit and Accountability Policy and Procedures

- IDVerifact shall establish a formal, documented audit and accountability policy and associated audit and accountability procedures.
- IDVerifact shall implement a process to review and update the audit and accountability policy and associated procedures at least annually.

Policy Supplement

A policy supplement has not been identified.

Guidance

ISO 27001:2005: Compliance with legal and contractual requirements

ISO 27001:2005: Compliance with security policies and standards

ISO 27001:2005: Technical compliance checking

Reference

1.2 Information System Audit Considerations

Purpose

The purpose of the IS Audit Considerations section is to establish controls and processes to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Policy

Information systems audit controls

- IDVerifact shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.

Protection of information systems audit tools

- IDVerifact shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.

Audit Events

- IDVerifact shall determine the type of events that are to be audited within information systems.
- IDVerifact shall review and update the list of audited events annually.
- IDVerifact leadership shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.

Content of Audit Records

- IDVerifact information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit Records Review and Reporting

- IDVerifact shall analyze information system audit records periodically.
- IDVerifact shall report findings of audit records reviews to information security personnel and IDVerifact leadership.
- IDVerifact shall perform correlation and analysis of information generated by security assessments and monitoring.

Policy Supplement

A policy supplement has not been identified.

Guidance

ISO 27001:2005: Information systems audit controls

ISO 27001:2005: Protection of information systems audit tools

1.3 Information Security Continuous Monitoring

Purpose	The purpose of the Information Security Continuous Monitoring policy is to establish controls that will provide IDVerifact effective monitoring and response capabilities in relation to compliance issues and incidents.
Policy	Continuous Monitoring • IDVerifact shall employ assessment teams to monitor the security controls on an ongoing basis. Plan of Action and Milestones • IDVerifact shall develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as a result of internal/external risk assessments, security reviews, and/or audits. • IDVerifact shall update its plan of action and milestones at least on a yearly basis and based on the findings from continuous security monitoring activities.
Policy Supplement	A policy supplement has not been identified.

IT Policy

1.0 Scope

1. Any employee, contractor or individual with access to Prodigy Labs and Prodigy Ventures systems or data.
2. Definition of data to be protected:
   1. Confidential emails
   2. Financial data
   3. Restricted or Sensitive data
   4. Confidential information
   5. Intellectual property

2.0 Policy - Employee requirements

1. If you identify an unknown, un-escorted or otherwise unauthorized individual in the IDVerifact office you need to immediately notify Human Resources.
2. Visitors to IDVerifact office should be always escorted by an authorized employee. If you are responsible for escorting visitors, you must restrict them to appropriate areas.
3. It is a requirement to not reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by Prodigy Labs/Prodigy Ventures. For example, the use of external email systems not approved by IDVerifact to distribute data is not allowed.
4. Please keep a clean desk. To maintain information security, you need to ensure that all printed in scope data is not left unattended at your workstation.
5. Prodigy Labs/Ventures endeavors to achieve a 100% paperless office environment. Print capability is limited to Human Resources and Finance. Only Authorized members

of those organizations have the ability to print paper copies, without approval. Members of these authorized groups are responsible for SOX and other Privacy compliance in accordance with the specific legislation.

6. All employees need a secure password on all IDVerifact systems as per the password policy (below). These credentials must be unique and must not be used on other external systems or services. IE same password for work email account vs personal email account.
7. Using 2FA (Two Factor Authentication) is a requirement and must be used on all services provided by Prodigy Labs\Ventures where available.
8. Terminated employees are required to return all records, in all formats, containing personal information. This includes physical devices, removable storage devices, and cloud storage locations.
9. You must notify the IT Operations Manager immediately in the event that a device containing in scope data is lost or stolen (e.g. Mobile Phones, Laptops etc.)
10. If you find a system or process which you suspect is not compliant with this policy or the objective of information security, you have a duty to inform the IT Operations Manager so that appropriate action can be taken.
11. In the event, appropriate action is not taken, or insufficient steps to mediate or remedy a security compliance violation, and/or such steps are taking an unreasonable amount of time, all Employees and Contractors are entitled and encouraged to escalate to IDVerifact CISO (Amanda Brooks), Sr Vice President (George Colwell), and President (Tom Beckerman) at any time.
12. Any information being transferred on a portable device (e.g. USB stick) must be encrypted in line with industry best practices. Client data is strictly prohibited from being transferred via removable or cloud storage unless explicitly approved by the Client.
13. All laptop hard drives are to have full disk encryption using (Bitlocker for PC’s and native full disk encryption for Mac’s)
14. You must ensure the lock screen is enabled when you are away from your desk. Do not leave your laptop or computer unattended and unlocked.
15. Passwords must be minimum of 8 characters and contain both numeric and alphanumeric characters with one uppercase, and one special character.
16. Passwords will be reset every 90 days.
17. All workstations must have a fully up to date anti-virus and anti-malware software.

3.0 Workstation Full Disk Encryption

Scope

1. All IDVerifact workstations - desktops and laptops
   Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements, impeding or blocking the running of business-critical applications) a risk assessment must be conducted being authorized by security management. Refer to the risk assessment process.

Policy

1. All devices in scope will have full disk encryption.
2. IDVerifact acceptable use policy requires users to notify the IT Operations Manager if they suspect they are not in compliance with this policy.

3. Encryptions policy must be managed, and compliance validated by IT Operations Manager. Machines need to report to the central management infrastructure to enable audit records to demonstrate compliance as required.
4. IDVerifact has the right to access any encrypted device for the purpose of investigation, maintenance, or the absence of an employee with primary file system access.
5. The encryption technology must be configured in accordance with industry best practices to be hardened against attacks.
6. All security-related events will be logged and audited by the IT Operations Manager to identify inappropriate access to systems or other malicious use.
7. Configuration changes are to be conducted through the change control process, identifying risks and noteworthy implementation changes to security management.

DEFINITIONS

Auditable event: A system activity identified by the entity's audit monitoring system that may be indicative of a violation of security policy. The activity may range from simple browsing to attempts to plant a Trojan horse or gain unauthorized access privilege.

Authentication: The process of establishing confidence in user identities through a well specified message exchange process that verifies possession of a password, token to remotely authenticate a claimant.

Authorization: Authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Authorization occurs within the context of authentication. Once a user has been authenticated, they may be authorized for different types of access.

Chief Information Officer: The agency official responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, information policies and information resources management responsibilities, including information security and the management of information technology.

Information owner: The person who has been identified as having the ownership of the information asset.

Information resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information resources manager (IRM): Responsible to the State of South Carolina for management of the [Agency]'s information resources. The designation of an [Agency] information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the [Agency]'s information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of South Carolina to implement security policies, procedures, practice standards, and guidelines to protect the information resources of the [Agency]. If the [Agency] does not designate an IRM, the title defaults to the [Agency]'s Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.